NUI Galway
OÉ Gaillimh

Autumn Examinations 2012/ 2013

Exam Code(s)	4IF1
Exam(s)	Bachelor of Science in Information Technology
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	
Repeat Paper	Yes
Discipline(s)	Information Technology
Course Co-ordinator(s)	
Internal Examiner(s)	Professor G Lyons Dr. M Madden Dr C Mulvihill*
External Examiner(s)	Professor M. O'Boyle
No. of Pages	3
Duration	**3 hours**
Instructions:	Attempt any four questions. All questions will be marked equally.

Requirements:
MCQ
Handout
Statistical/ Log Tables
Cambridge Tables
Graph Paper
Log Graph Paper
Other Materials

Release to Library: Yes

PTO

1

(a) Describe the process of capturing information from a suspect PC using the headings (1) sanitizing the forensic disk (2) imaging the suspect disk (3) disk analysis (8 marks)

(b) Discuss the importance of trustworthy (received:) headers in email (6 marks)

(c) A suspect disk contains a scrubbing program. In your opinion does this mean that all hope of recovering any data whatsoever is gone? (6 marks)

2

(a) Give any three properties that a hash function should satisfy (6 marks)

(b) Outline the number theory that underlies an RSA asymmetric encryption scheme, explaining what is meant by Euler's totient (or Phi) function in the course of your discussion (8 marks)

(c) Give your understanding of the term ‘freshness’ (6 marks)

3

(a) Give your understanding of Public Key Infrastructure using the headings (1) Registration Authority (2) Certification Authority (3) Certificate Revocation List (4) Public and private keys (8 marks)

(b) You are told that a certificate is untrusted. What does this mean? (6 marks)

(c) Tom has hashed a file for 'authentication purposes' and then encrypted this file with Mary's public key for 'confidentiality purposes'. Tom believes that he can still decrypt this message. Advise on this particular use of hashes and keys. (6 marks)

4

(a) Discuss any three areas that you would expect to be addressed in a typical corporate security policy document for an SME. (6 marks)

(b) Your company has decided to pilot a two-factor authentication scheme. Explain what this means (6 marks)

(c) You are to provide advice on security policy in an organisation. The organisation prizes data integrity above all else. Discuss what read/write policy you might consider appropriate for this environment (8 marks)

PTO

5

(a) Explain what is meant by the terms (1) Confidentiality (2) Integrity and (3) Availability (6 marks)

(b) In an hierarchical environment that prizes confidentiality above all else, discuss what read/write policy you might expect to find in place. (8 marks)

(c) Give your understanding of the term 'Chinese wall' (6 marks)

6

(a) Discuss any one problem that Solid State Drive technology poses for current forensic practice (8 marks)

(b) A suspect claims that they cannot remember the password for an encrypted file. Discuss any three options that may be available to you as an investigator (6 marks)

(c) You are tasked with outlining to staff how an ARP cache poisoning attack works. Briefly outline the main points that you would expect to make in connection. (6 marks)

7

"Smartphones and social networking have almost eliminated privacy for many people." Discuss this statement. (20 marks)